要約書 (Abstract)

暗号文に関しての強度の評価を行う暗号強度評価装置が、複数攪拌段階の拡大鍵をまとめて求めるに関して計算量等の削減を行うことを目的とし、暗号強度評価装置に、鍵より算出され、暗号化のある攪拌段階で用いられる拡大鍵に等しいと推定される拡大鍵候補の一つをまず算出させ、この拡大鍵候補を正しいと仮定することで次に復号化操作を行わせ、得られた文に基づいて当該前攪拌段階の拡大鍵候補を算出させることで異なる段階の拡大鍵を続けて算出させ、早期に複数の正しい拡大鍵候補を算出させられる可能性を高めた。